UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

MARC LAGASSE and ANDREA E. PETRUNGARO, individually and on behalf of all others similarly situated,	:	17-cv- _____ ( )
Plaintiffs,	:	
v.	:	**CLASS ACTION COMPLAINT**
EQUIFAX INC. and EQUIFAX INFORMATION SERVICES, LLC,	:	
Defendants.	:	
	:	JURY TRIAL DEMANDED

Plaintiffs Marc LaGasse and Andrea E. Petrungaro, individually and on behalf of those similarly situated, hereby file this Complaint against Defendants Equifax Inc. and Equifax Information Services, LLC (collectively "Equifax"). In support thereof, Plaintiffs state as follows:

NATURE OF THE ACTION

1. This is a suit seeking to remedy perhaps the most significant data breach in history.

2. Equifax collects, stores, and sells data about consumers' credit.

3. That data is some of the most important, sensitive data that consumers possess – credit card numbers, Social Security numbers, and other data that, when stolen, causes consumers significant financial damage.

4. Because of the sensitive nature of this data – and the significant harm caused by theft of this data – Equifax has statutory and common-law duties to take reasonable actions to secure the data that it collects.

5. Equifax breached its duties to secure consumers' data. Security experts had for months been warning of a specific problem – an "exploit" – in software behind Equifax's public website. Fixing the problem would have required only applying a widely available "patch" or implementing one of several other publicly disclosed alternatives. But Equifax did not implement the patch – a failure analogous to not changing your locks after you learn that your keys are being distributed publicly.

6. Unfortunately, but unsurprisingly, criminals exploited the flaws in Equifax's systems and over ***at least two months*** stole massive amounts of consumer data. As a result, the sensitive data of approximately 143 million Americans has now been exposed to identity thieves and other unsavory characters.

7. Incredibly, Equifax waited months to provide notice to the victims of the theft.

8. To add insult (and further injury) to injury, Plaintiffs and other members of the Class must now pay fees to "freeze" their credit and must also pay other credit bureaus to monitor their credit more closely. Moreover, with their most sensitive financial data now exposed to criminals, the Class also now faces significantly elevated risks of identity theft.

9. Accordingly Plaintiffs bring this action on behalf of themselves and others similarly situated to obtain redress and to hold Equifax responsible for losses caused by its failure to adequately safeguard the Class's data.

THE PARTIES

10. Plaintiff Marc LaGasse is a resident and citizen of the state of Illinois. Mr. LaGasse is among the 143 million Americans whose data was compromised in the Equifax data breach.

11. Plaintiff Andrea E. Petrungaro is a resident and citizen of the state of Illinois. Ms. Petrungaro is also among the 143 million Americans whose data was compromised in the Equifax data breach.

12. Defendant Equifax Inc. is a Georgia corporation with a principal office address of 1550 Peachtree Street NW, H46, Atlanta, GA, 30309.

13. Defendant Equifax Information Services, LLC is a Georgia limited liability company with a principal office address of 1550 Peachtree Street NW, H46,

Atlanta, GA, 30309. Upon information and belief, Equifax Information Services, LLC's sole member is Equifax Inc.

14. Defendants Equifax Inc. and Equifax Information Services, LLC (together "Equifax" or Defendants) are one of the three major consumer credit reporting agencies in the United States. On information and belief, Equifax Information Services, LLC manages the Equifax consumer credit report business and Equifax Inc. operates the server infrastructure that hosts the personal data stolen in the data breach that forms the basis for this Complaint.

JURISDICTION AND VENUE

15. This Court has diversity jurisdiction over Plaintiffs' claims pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d). At least one member of both the Nationwide and Illinois State Classes is of diverse citizenship from Defendant, damages are over $5,000,000, exclusive of interest and costs, and each Class contains more than 100 members.

16. This Court also has federal question jurisdiction under 28 U.S.C. § 1331 because Plaintiffs bring claims arising under the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681e, et seq., and supplemental jurisdiction over the state-law claims under 28 U.S.C. § 1367(a).

17. This Court has personal jurisdiction over Equifax Inc. because Equifax Inc. is a Georgia corporation and it has its principal office in Atlanta, Georgia.

18. This Court has personal jurisdiction over Equifax Information Services, LLC, because Equifax Information Services, LLC's principal place of business is in Atlanta, Georgia and because, on information and belief, its sole member is Equifax Inc., a Georgia corporation with its principal place of business in Atlanta, Georgia.

19. Venue is proper in this District under 28 U.S.C. § 1391(b)(1) and (b)(2), because Defendants' principal place of business is in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL BACKGROUND

I. Equifax Collects and Stores the Most Sensitive Consumer Data

20. Equifax has collected and currently stores at least some sensitive data for the ***majority*** of all Americans; it advertises its "access to current personally identifiable information for over 210 million consumers"[1] and that it "organizes,

[1] *Product Overview*, EQUIFAX INC., http://www.equifax.com/business/consumer-reports (last visited Sept. 20, 2017).

assimilates, and analyzes data on more than 820 million consumers . . . worldwide."[2]

21. The data that Equifax collects and sells is incredibly sensitive, personal data linked to consumers, including Social Security numbers, dates of birth, addresses, payment histories, and account numbers. This data includes data about consumers' "credit, financial assets, telecommunications and utility payments, employment, income, [and] demographic and marketing data."

22. This data must be safeguarded. It is widely acknowledged that the theft of the data stored by Equifax causes significant harm. For example, a 2008 report from the Government Accountability Office noted that the loss of such data "can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information."[3]

23. Similarly, a White House report from earlier this year noted that, when stolen, consumer data can result in "financial- or credit-related identity theft such as using a stolen credit card number, opening a new bank account, or applying for credit

---

[2] *Cybersecurity Incident & Important Consumer Information*, EQUIFAX INC., https://www.equifaxsecurity2017.com/ (last visited Sept. 20, 2017).

[3] U.S. GOV'T ACCOUNTABILITY OFF., GAO-08-343, INFORMATION SECURITY 18 (2008).

in another person's name." "[M]alicious actors" also use stolen consumer data to "seek employment, . . . file false tax returns, and aid in other criminal activities." [4]

24. Those harms are felt for ***years*** after the data is initially stolen. "Years after personal data is leaked, identity theft victims have faced ***financial ruin***."[5] "Identity thieves plunder people's credit, riddling their credit reports with false information including debts and second mortgages obtained in their names."[6] Thieves might use the data at any time, leaving victims exposed to financial hardship for literally the rest of their lives.[7]

25. The importance of keeping this data confidential is also underscored by numerous statutes and regulations that require Equifax to protect it.

---

[4] Memorandum from Exec. Off. of the President to Heads of Exec. Depts. and Agencies. 5-6 (Jan 3, 2017) (https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf).

[5] Daniel J. Solove and Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 Texas. L.R. _ (2017) (emphasis added).

[6] *Id.*

[7] Andrea Peterson, *Data Exposed in Breaches Can Follow People Forever*, WASH. POST, June 15, 2015. http://www.washingtonpost.com/blogs/the-switch/wp/2015/06/15/data-exposed-in-breaches-can-follow-people-forever-the-protections-offered-in-their-wake-dont/ (last visited Sept. 20, 2017).

26. For example, the Gramm-Leach-Bliley Act was specifically designed to "[p]rotect against any anticipated threats or hazards to the security or integrity of [consumer] information" and "protect against unauthorized access to or use of such information." 16 C.F.R. § 314.3(b)(2)-(3).

27. The protection of consumer data is so important that the Gramm-Leach-Bliley Act ***requires*** financial institutions to "develop, implement, and maintain ***a comprehensive information security program***" with "administrative, technical, and physical safeguards that are appropriate to . . . the sensitivity of any customer information at issue." 16 C.F.R. § 314.3(a) (emphasis added).

28. The security program required by Gramm-Leach-Bliley must anticipate threats. Financial institutions must "[i]dentify reasonably ***foreseeable internal and external risks to the security***, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks." 16 C.F.R. § 314.4(b) (emphasis added).

29. The Gramm-Leach-Bliley Act requires financial institutions to "[d]esign and implement information safeguards to control the risks [they] identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures." 16 C.F.R. § 314.4(c).

30. Especially relevant here – once a financial institution learns of a threat to its security, it must take steps to address it. Gramm-Leach-Bliley requires financial institutions to "[e]valuate and adjust [their] information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; [and] . . . any other circumstances that [they] ***know or have reason to know*** may have a material impact on [their] information security program." 16 C.F.R. § 314.4(e) (emphasis added).

31. Another act, the Fair Credit Reporting Act ("FCRA"), also underscores the importance of protecting consumer data by requiring consumer reporting agencies – like Equifax – to safeguard consumers' personal data.

32. Congress, in enacting FCRA, found that "[c]onsumer reporting agencies," like Equifax, "have assumed a vital role in assembling and evaluating consumer credit and other information on consumers" and, as a result, "[t]here is a need to insure that consumer reporting agencies exercise their ***grave responsibilities*** with . . . a respect for ***consumer's right to privacy***." 15 U.S.C. § 1681(a)(3)-(4) (emphasis added).

33. Accordingly, under FCRA, Equifax may only disclose a consumer's data in limited circumstances – *e.g.*, when a reputable financial institution seeks to verify a consumer's data before extending credit to that consumer.

34. But FCRA requires Equifax to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports" for proper purposes to entities that need the data to assess consumer credit. 15 U.S.C. § 1681e(a). FCRA prohibits Equifax from disclosing consumers' valuable data to hackers, thieves, and other ne'er-do-wells.

35. Finally, the Federal Trade Commission ("FTC") has also recognized the importance of the consumer data that Equifax stores. Under the FTC's interpretations of the FTC Act, the failure to "provide reasonable and appropriate security for the sensitive personal information on [an entity's] computer network" violates Section 5 when the "failure caused or was likely to cause substantial injury that consumers could not have reasonably avoided and that was not outweighed by benefits to consumers or competition." *In the Matter of LabMD, Inc.*, F.T.C. No. 9357, Trade Reg. Rep. P 79708 (C.C.H.), 2016 WL 5821739 (July 28, 2016).

36. The federal government is not alone in recognizing the need to safeguard the data that Equifax stores. State laws in Illinois also recognize the critical importance of keeping that data safe and impose a duty on Equifax to safeguard personal data.

37. The Illinois Personal Information Protection Act ("PIPA") specifically protects an individual's Social Security number, driver's license, and account numbers (like credit cards and bank accounts).

38. Under PIPA, "[a] data collector," like Equifax, "that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall ***implement and maintain reasonable security measures to protect those records from unauthorized access***, acquisition, destruction, use, modification, or disclosure." 815 ILCS 530/45 (emphasis added).

39. Additionally, recognizing the importance of quick corrective action once a breach occurs, PIPA requires data collectors like Equifax to provide notice "in the most expedient time possible and without unreasonable delay" of any data breach or theft of personal data. 815 ILCS 530/10.

40. The importance of safeguarding consumer data comes as no surprise to Equifax, which has long acknowledged that it has a duty to keep this data safe.

41. For example, in its 2016 annual report, filed on February 22, 2017, Equifax explicitly noted that it is "subject to various [Gramm-Leach-Bliley (GLB) Act] provisions, including rules relating to the use or disclosure of the underlying

data and rules relating to the physical, administrative and technological protection of non-public personal financial information."[8]

42. In the same annual report, Equifax acknowledged that "[t]he security measures [it] employ[s] to safeguard the personal data of consumers could also be subject to the [Federal Trade Commission] Act, and failure to safeguard data adequately may subject [Equifax] to regulatory scrutiny or enforcement action."[9]

43. Equifax also noted that "[a] majority of states have adopted versions of data security breach laws that require notification of affected consumers in the event of a breach of personal information. Some of these laws require additional data protection measures which exceed the GLB Act data safeguarding requirements. If data within our system is compromised by a breach, we may be subject to provisions of various state security breach laws."[10]

II. Despite Its Acknowledged Duties, Equifax Has Repeatedly Permitted Thieves To Steal Consumers' Data

44. Despite the sensitivity of the data Equifax stores and sells, and the duties Equifax itself acknowledged, Equifax consistently cut corners in its data

---

[8] Equifax Inc., Annual Report (Form 10-K) at 10 (Feb. 22, 2017).

[9] *Id.*

[10] *Id.* at 11.

security practices and maintained a culture of lax security. This has led to numerous thefts of data from Equifax, including:

- In 2013, Equifax credit reports were stolen from the company in a high-profile unauthorized-access incident, including Social Security numbers and banking data for Michelle Obama, Joe Biden, Donald Trump, and others.[11]
- In March 2014, an individual or entity located at a specific static IP address had been repeatedly able to fool the Equifax identity verification process and obtain unauthorized credit reports over a period of nearly a year, without being detected, between April 2013 and January 31, 2014.[12]

---

[11] Pierre Thomas, *Equifax Confirms Hackers Stole Financial Data, Launches Investigation*, ABC NEWS, http://abcnews.go.com/Politics/equifax-confirms-hackers-stole-financial-data-launches-investigation/story?id=18715884 (last visited Sept. 20, 2017).

[12] Letter from Troy G. Kubes, V.P. & Assoc. Group Counsel, Equifax Legal Dept. to Joseph Foster, Att'y. Gen. N.H. (Mar. 5, 2014) (https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20140305.pdf).

- In 2016, hackers obtained W-2 data for thousands of people from Equifax's websites simply by entering the last four digits of the employees' Social Security numbers and their four-digit birth years.[13] [14]
- From April 2016 to March 2017, hackers obtained unauthorized access to personal data for an unknown number of individuals from an Equifax subsidiary.[15] In response, security researchers called Equifax's security "lax" and "unbelievable."[16]

45. One would suppose that this history of security breaches would inspire

---

[13] Brian Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*, KREBS ON SECURITY, https://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/ (last visited Sept. 20, 2017).

[14] Russell Grantham, *Equifax sued over theft of Kroger workers' info*, AJC.COM, https://www.ajc.com/business/equifax-sued-over-theft-kroger-workers-info/cjwGCYI8bkCg1fFIRri93H/ (last visited Sept. 20, 2017).

[15]Letter from Nicholas A. Oldham, Counsel for TALX Corp. to Joseph Foster, Attn'y Gen. N.H. (May 15, 2017) (https://www.doj.nh.gov/consumer/security-breaches/documents/talx-20170515.pdf).

[16] Brian Krebs, *Fraudsters Exploited Lax Security at Equifax's TALX Payroll Division*, KREBS ON SECURITY, https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/ (last visited Sept. 20, 2017).

Equifax to shore up its systems – ***especially*** against known or obvious vulnerabilities. But to this day, researchers and reporters continue to note basic flaws in Equifax's security.

46. In September 2017, security researchers commented that Equifax's "approach to security was just abysmal"[17] and with "security vulnerabilit[ies]" that are "extraordinary" and that "even the most basic of checks should reveal."[18] These flaws included:

- that certain Equifax servers used "admin/admin" as the administrator username and password – defying basic common sense and contradicting security that even grade-school users of computers know and implement;
- and that some Equifax servers stored and displayed each Equifax employee's individual password in plain text (and, in each instance, each password was identical to the employee's username).

---

[17] Brian Krebs, *Ayuda! (Help!) Equifax Has My Data!*, KREBS ON SECURITY, https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/ (last visited Sept. 20, 2017).

[18] *Equifax had 'admin' as login and password in* Argentina, BBC NEWS, http://www.bbc.com/news/technology-41257576 (last visited Sept. 20, 2017).

47. Equifax continues to leave itself open to security threats. On September 12, the technology website ZDNet advised that because of an unresolved website vulnerability, readers should not enter their personal data into the Equifax credit freeze website because doing so risked having their data stolen. A security expert quoted in the article described the vulnerability as one that "enables an attacker to run their own arbitrary [code] in a victim's browser," enabling them to "grab[ ] any information entered into the page" and "even deliver malware to the victim." The expert found the flaw "alarming" but said "even more alarming is that the researcher [who identified the issue] hasn't been able to get a response when attempting to report it."[19]

48. Another vulnerability of the same type had been reported in March 2016.[20] According to Open Bug Bounty, that vulnerability was not patched until

---

[19] Zack Whittaker, *Equifax's credit report monitoring site is also vulnerable to hacking*, ZERO DAY, http://www.zdnet.com/article/equifax-freeze-your-account-site-is-also-vulnerable-to-hacking/ (last visited Sept. 20, 2017).

[20] Chris Brook, *Many Questions, Few Answers for Equifax Breach Victims*, THREATPOST.COM, https://threatpost.com/many-questions-few-answers-for-equifax-breach-victims/127886/ (last visited Sept. 20, 2017).

September 9 of this year – ***a year and a half after it was reported***.[21]

49. Security researchers have also faulted Equifax for running legacy and outdated software. One researcher noted that even "a cursory glance at Equifax's network revealed the company was running a handful of legacy systems that may have contributed"[22] to the risk of a breach. Another said that the software running on the main Equifax website is "like stepping back in time a decade."[23] A third pointed out that "[i]t really looks like they don't care about security on their website – not surprised they got breached, certainly easy."

III. Equifax's Lax Security Gave Hackers Continual Access to Plaintiffs' and Class Members' Data from at Least Mid-May 2017 Through July 2017

50. Equifax's failure to fix security issues it knew or reasonably should have known about led directly to the theft of Plaintiffs' and Class members' data.

51. Specifically, Equifax employed a framework called "Apache Struts" for certain web applications. A vulnerability in Apache Struts permitted hackers

---

[21] *Equifax.com Security Vulnerability*, OPENBUGBOUNTY.ORG, https://www.openbugbounty.org/reports/141440/ (last visited Sept. 20, 2017).

[22] Brook, s*upra* n.20.

[23] Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, FORBES, https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#638b1b3a677c (last visited Sept. 20, 2017).

unrestricted access to Plaintiffs' and Class members' data from at least mid-May 2017 through July 2017.

52. The vulnerability was well known, and Equifax could have addressed it in time to prevent the hack.

53. Around March 6, 2017, Apache Struts issued a security bulletin informing users of the "Critical" security flaw, which would permit a malicious attacker to execute remote code. The bulletin gave users multiple options to address the flaw.

54. The U.S. government's United States Computer Emergency Readiness Team (US-CERT) issued a public warning of the vulnerability at around the same time.

55. Major information technology news media sources soon began reporting escalating attacks based on this security flaw. A March 9, 2017 article in PCWorld reported, "Attackers are widely exploiting a recently patched vulnerability in Apache Struts that allows them to remotely execute malicious code on web servers."[24] An Ars Technica article titled *Critical vulnerability under "massive"*

[24] Lucian Constantin, *Hackers exploit Apache Struts vulnerability to compromise corporate web servers*, PC WORLD (Mar. 9. 2017 at 3:53 AM PT),

attack imperils high-impact sites reported the same day that "hackers are actively exploiting a critical vulnerability that allows them to take almost complete control of Web servers used by banks, government agencies, and large Internet companies."[25] The article warned that "[o]utside researchers . . . have said the exploits are trivial to carry out, are highly reliable, and require no authentication."[26] A Bank Info Security article also on March 9 urged readers "Update Now," warning that "Apache Struts 2 installations are being targeted – and hacked in large numbers."[27]

56. According to Equifax's September 15 statement, "Equifax's Security organization was aware of this vulnerability" in early March 2017.

---

https://www.pcworld.com/article/3178660/security/hackers-exploit-apache-struts-vulnerability-to-compromise-corporate-web-servers.html.

[25] Dan Goodin, *Critical vulnerability under "massive" attack imperils high-impact sites*, ARS TECHNICA (Mar. 9. 2017 at 12:07 PM), https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/.

[26] *Id.*

[27] Mathew J. Schwartz, *Apache Struts 2 Under Zero-Day Attack*, BANK INFO SECURITY (Mar. 9, 2017), https://www.bankinfosecurity.com/apache-struts-2-under-zero-day-attack-update-now-a-9761.

57. Despite the widespread knowledge of the Apache Struts problem – including at Equifax – Equifax failed to close this security hole until the data breach was discovered around July 29, 2017 – nearly five months after the patch was released and major attacks were reported in the media. By then it was too late. Hackers had been stealing consumer data for months.

58. The hack was all the more successful – and all the more damaging to consumers – because of other flaws in Equifax's security practices. For example, Equifax stored sensitive consumer data in public-facing web applications – the electronic equivalent of a bank removing valuables from a safety-deposit box and putting them in tellers' drawers. Hence, once hackers had exploited Equifax's security, they had easy access to a rich trove of highly sensitive data.

59. To make matters still worse, Equifax also failed to employ reasonable intrusion detection and monitoring measures that would have been capable of detecting the attack in progress. If Equifax had some kind of reasonable detection system, it might have been able to stop the hack quickly. Instead, hackers thus had unrestricted access to sensitive consumer data for over two months – if not longer.

60. The sum total of these failures – not applying a critical, known patch; leaving consumer data in an easily accessible place; and failing to detect the hack quickly – had disastrous consequences.

61. Criminals accessed the data of approximately ***143 million*** Americans. By Equifax's own admission, "[t]he information accessed" is highly sensitive, and includes Social Security numbers, driver's license numbers, birth dates, credit card numbers, and other sensitive data.

62. And yet, Equifax still managed to make matters worse yet. Despite learning of the data breach in July 2017, Equifax did not inform consumers that their data had been stolen until September 2017.

63. It appears, however, that Equifax knew immediately that the data breach was significant. In the days after the intrusion was discovered, three senior Equifax executives sold between 4 and 13 percent of their Equifax shareholdings.

IV. Plaintiffs and Class Members Have and Will Continue to Suffer Injury Due to Equifax's Lax Security

64. Data breaches cause significant harm to victims. "Victims struggling with identity theft have been forced to file for bankruptcy, and some have lost their homes."[28] They can be "turned down for loans or end up paying higher interest rates

[28] Solove, *supra* at 14.

on credit cards."[29] "On average, it takes up to thirty hours to resolve problems when identity thieves open new accounts in victims' names."[30]

65. The Equifax data breach is no different. It has caused and will continue to cause serious harm to the Plaintiffs and the Class.

66. Plaintiffs and the Class members must pay out-of-pocket costs to minimize their future losses.[31] For example, after learning that her data had been exposed in the Equifax data breach, Ms. Petrungaro paid to "freeze" her credit, thereby making it more difficult for a thief to obtain credit in her name. Plaintiffs must also pay for ongoing credit monitoring. For example, after learning that his data had been exposed in the Equifax data breach, Mr. LaGasse purchased a subscription to a credit monitoring service, which includes an identity theft alert and account monitoring.

67. In addition to the out-of-pocket costs of paying for the credit freezes, Plaintiffs who have paid to "freeze" their credit must now contact the credit bureaus well in advance of opening a new line of credit and undertake a special process,

---

[29] *Id.*

[30] *Id.* at 14-15.

[31] *Id.* at 15 ("Data breach victims incur out of pocket costs to minimize future losses.").

including payment of an additional fee, to unfreeze their credit. This will generally make it more burdensome for Plaintiffs to obtain credit and represents an opportunity cost to Plaintiffs.

68. Notwithstanding those efforts to minimize losses, other damage is accruing. Plaintiffs and the Class are at risk for fraud for years to come. As one expert has noted, "Social Security Numbers have a very long shelf life -- a bad guy that's smart won't use it immediately, he'll keep a hoard of numbers and use them in a couple of years."[32]

69. Plaintiffs and Class members thus have suffered and will continue to suffer injury, including: (a) costs incurred, and that will be incurred, in time and money for the monitoring of their credit reports and financial accounts to become aware of any fraud or identity theft; (b) costs incurred, and that will be incurred, for freezing and unfreezing credit reports with the three major credit bureaus so that identity thieves are less easily able to open new accounts in their names; and (c) increased risk of identity theft.

[32] Peterson, *supra*.

CLASS ACTION ALLEGATIONS

70. Plaintiffs bring all claims as class claims under Federal Rule of Civil Procedure Rule 23(b)(1), (b)(2), (b)(3), and (c)(4).

71. Plaintiffs bring their FCRA and Negligence claims (Counts I, II, III, & IV) on behalf of a proposed nationwide class ("Nationwide Class"), defined as follows:

> All natural persons and entities in the United States whose personal data was exposed to unauthorized persons in the data breach announced by Equifax in September 2017.

72. Plaintiffs also bring their Negligence and Illinois Consumer Fraud and Deceptive Business Practices Act claims (Counts III, IV, and V) on behalf of a proposed class of Illinois residents ("Illinois State Class"), defined as follows:

> All natural persons and entities in Illinois whose personal data was exposed to unauthorized persons in the data breach announced by Equifax in September 2017.

73. Excluded from the Nationwide Class and the Illinois State Class are Defendants and their current employees, as well as the Court and its personnel presiding over this action.

74. The Nationwide and Illinois State Classes meet the requirements of Federal Rule of Civil Procedure 23.

75. **Numerosity—Federal Rule of Civil Procedure 23(a)(1):** The members of the Class are so numerous that joinder of all Class members would be impracticable. Although the exact number of Class members is unknown to Plaintiffs at this time, the proposed Class may include approximately 143 million individuals whose data was compromised in the Equifax data breach.

76. **Commonality and Predominance—Fed. R. Civ. P. 23(a)(2) and (b)(3)**: This action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include, *inter alia*:

a. whether Defendants engaged in the wrongful conduct alleged herein;

b. whether Defendants had a duty to protect consumer data;

c. whether Defendants failed to use reasonable care to protect and secure Plaintiffs' and the Class members' data;

d. whether Defendants violated FCRA;

e. whether Plaintiffs and Class members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and out-of-pocket expenses to guard against that risk; and

f. whether Plaintiffs and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

77. **Typicality—Fed. R. Civ. P. 23(a)(3):** Plaintiffs' claims are typical of the claims of the Class. Each of the Plaintiffs, like all proposed Class members, had personal data compromised in the data breach.

78. **Adequacy—Fed. R. Civ. P. 23(a)(4):** Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs have no interests that are adverse to, or in conflict with, the Class members. There are no claims or defenses that are unique to Plaintiffs. Plaintiffs have retained counsel experienced in complex litigation and class action litigation that have sufficient resources to prosecute this action vigorously.

79. **Superiority—Fed. R. Civ. P. (23)(b)(3):** The proposed action also meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions is superior to multiple individual actions or piecemeal litigation, avoids inconsistent decisions, presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member. Absent a class action, the

majority of Class members would find the cost of litigating their claims prohibitively high and would have no effective remedy.

80. **Risks of Prosecuting Separate Actions—Fed. R. Civ. P. 23(b)(1):** Plaintiffs' claims also meet the requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Equifax. Equifax continues to maintain the data of the Class members and other individuals, and varying adjudications could establish incompatible standards with respect to Equifax's duty to protect individuals' data. Prosecution of separate actions by individual Class members would also create a risk of individual adjudications that would be dispositive of the interests of other Class members not parties to the individual adjudications, or substantially impair or impede the ability of Class members to protect their interests.

81. **Certification of Particular Issues—Fed. R. Civ. P. 23(c)(4):** In the alternative, the Nationwide Class and Illinois State Class may be maintained as class actions with respect to particular issues, in accordance with Federal Rule of Civil Procedure 23(c)(4). In particular, any of the common issues identified in paragraph 76 are susceptible to class treatment pursuant to Rule 23(c)(4).

82. **Injunctive Relief—Fed. R. Civ. P. 23(b)(2):** In addition, Equifax has acted or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Federal Rule of Civil Procedure 23(b)(2). Equifax continues to (1) maintain Plaintiffs' and the Class members' data, (2) fails to adequately protect that data, and (3) violates the Plaintiffs' and the Class members' rights under the FCRA and other claims alleged herein.

COUNT I – WILLFUL VIOLATIONS OF THE FAIR CREDIT REPORTING ACT
(On Behalf of the Nationwide Class)

83. Plaintiffs and the Class members incorporate and reallege Paragraphs 1 through 82 of the Complaint as if fully set forth herein.

84. As individuals, Plaintiffs and Class members are consumers entitled to the protections of the FCRA, 15 U.S.C. § 1681a(c).

85. Equifax is a consumer reporting agency under FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit data or other data on consumers for the purpose of furnishing consumer reports to third parties.

86. Communications on Equifax's servers that contain personal data such as Social Security numbers, birth dates, driver's license numbers, addresses, credit

card numbers, and credit report disputes are "consumer reports" under the FCRA because they constitute "communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, . . . personal characteristics, or mode of living which is . . . collected in whole or in part for the purpose of serving as a factor in establishing" credit. 15 U.S.C. §1681a(d)(1).

87. Equifax willfully violated the FCRA by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports for purposes not authorized by 15 U.S.C. § 1681b, in violation of 15 U.S.C. § 1681e(a).

88. Equifax willfully violated the FCRA by providing impermissible access to consumer reports, in violation of 15 U.S.C. § 1681b. The willful nature of Equifax's violations is supported by, among other things, Equifax's numerous other data breaches in the past and its failure to respond to known security exploits, including the one that caused the data breach.

89. Equifax also acted willfully because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching

known duties regarding data security and data breaches and depriving Plaintiffs and other Class members of their rights under the FCRA.

90. Equifax's willful conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Class members' personal data for no permissible purposes under the FCRA.

91. Plaintiffs and the Class members have been damaged by Equifax's willful failure to comply with the FCRA. Therefore, Plaintiffs and each of the Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than $100 and not more than $1,000." 15 U.S.C. § 1681n(a)(1)(A).

92. Plaintiffs and the Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2) & (3).

COUNT II – NEGLIGENT VIOLATIONS OF THE FAIR CREDIT REPORTING ACT
(On Behalf of the Nationwide Class)

93. Plaintiffs and the Class members incorporate and reallege Paragraphs 1 through 92 of the Complaint as if fully set forth herein.

94. Equifax negligently failed to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA.

95. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, Equifax's numerous other data breaches in the past and its failure to respond to known security exploits, including the one that caused the data breach.

96. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class members' personal data and consumer reports for no permissible purposes under the FCRA, thereby damaging Plaintiffs and the Nationwide Class.

97. Therefore, Plaintiffs and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. §1681o(a)(1). Plaintiffs and the Nationwide Class members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. §1681o(a)(2).

COUNT III – NEGLIGENCE
(On behalf of the Nationwide Class and the Illinois State Class)

98. Plaintiffs and the Class members incorporate and reallege Paragraphs 1 through 97 of the Complaint as if fully set forth herein.

99. Defendants owe a common-law duty to Plaintiffs and the Class members to exercise reasonable care in collecting, storing, and making their personal

data available for sale, including the duty to use reasonable technological security measures to safeguard personal data from unauthorized access.

100. Defendants breached this duty by, among other things: (a) failing to implement adequate security protocols and practices; (b) failing to layer their security so as to prevent a security hole in a public-facing website from granting hackers access to millions of consumers' personal data; (c) failing to patch or implement a workaround for the CVE-2017-5638 exploit in a timely manner; (d) failing to monitor their public-facing servers so as to be able to recognize and stop the intrusion after it had begun; and (e) failing to notify Plaintiffs and Class members of the data breach in a timely manner.

101. But for Equifax's negligent breaches of duty owed to Plaintiffs and the other Class members, the personal data would not have been stolen and the Plaintiffs and Class members would not have been injured, or the Plaintiffs and Class members would have been able to take protective action sooner, improving their chances of preventing fraud and identity theft due to the sale of their personal data.

102. Defendants' inadequate protection of consumers' personal data was the proximate cause of the data breach resulting in the theft of the Plaintiffs' and Class members' data.

103. Plaintiffs and the Class members suffered injury as a result of Defendants' negligence.

104. Defendants acted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT IV – NEGLIGENCE PER SE
(On behalf of the Nationwide Class and the Illinois State Class)

105. Plaintiffs and the Class members incorporate and reallege Paragraphs 1 through 104 of the Complaint as if fully set forth herein.

106. Defendants are obligated to safeguard consumers' personal data under the Gramm-Leach-Bliley Act and rules promulgated thereunder, the FTC Act, the FCRA, and state consumer and privacy statutes including the Illinois Consumer Fraud and Deceptive Trade Practices Act and the Illinois Personal Information Protection Act.

107. Defendants violated these statutes by, among other things: (a) failing to implement adequate security protocols and practices; (b) failing to layer their security so as to prevent a security hole in a public-facing website from granting hackers access to millions of consumers' personal data; (c) failing to patch or implement a workaround for the CVE-2017-5638 exploit in a timely manner; (d) failing to monitor their public-facing servers so as to be able to recognize and stop

the intrusion after it had begun; and (e) failing to notify Plaintiffs and Class members of the data breach in a timely manner.

108. Plaintiffs and Class members are within the class of persons the Gramm-Leach-Bliley Act, the FTC Act, the FCRA, and state consumer and privacy statutes are intended to protect.

109. The theft of personal data and the resulting injuries are within the class of harms the Gramm-Leach-Bliley Act, the FTC Act, the FCRA, and state consumer and privacy statutes are intended to protect against.

110. Defendants' violations of the Gramm-Leach-Bliley Act and rules promulgated thereunder, the FTC Act, the FCRA, and state consumer and privacy statutes thus constitute negligence per se.

111. But for Equifax's violations of the Gramm-Leach-Bliley Act and rules promulgated thereunder, the FTC Act, the FCRA, and state consumer and privacy statutes, the personal data would not have been stolen and the Plaintiffs and Class members would not have been injured, or the Plaintiffs and Class members would have been able to take protective action sooner, improving their chances of preventing fraud and identity theft due to the sale of their personal data.

112. Defendants' inadequate protection of consumers' personal data was the proximate cause of the data breach resulting in the theft of the Plaintiffs' and Class members' data.

113. Plaintiffs and the Class members suffered injury as a result of Defendants' negligence.

114. Defendants also acted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

COUNT V – VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
(On behalf of the Illinois State Class)

115. Plaintiffs and the Class members incorporate and reallege Paragraphs 1 through 114 of the Complaint as if fully set forth herein.

116. Plaintiffs' personal data is Personal Information under the Illinois PIPA, because names, Social Security numbers, credit card numbers, and driver's license numbers were included.

117. Defendants are data collectors under the Illinois PIPA, since they are financial institutions or other entities that "for any purpose, handle[ ], collect[ ], disseminate[ ], or otherwise deal[ ] with nonpublic personal information." 815 ILCS 530/5.

118. Defendants failed to implement and maintain reasonable security measures to protect the personal data from unauthorized access, acquisition, destruction, use, modification, or disclosure, as required by the Illinois PIPA. Defendants' violation of PIPA is an unlawful act under the Illinois Consumer Fraud and Deceptive Business Practices Act.

119. Additionally, Defendants own or license information concerning Illinois residents and were required to notify residents of the breach in accordance with the Illinois PIPA.

120. Defendants failed to notify Plaintiffs and Class members of the data breach in the most expedient time possible and without unreasonable delay, in violation of PIPA. Defendants' failure to provide timely notice of the data breach is thus an additional unlawful act under the Illinois Consumer Fraud and Deceptive Business Practices Act.

121. Defendants' violation of the Illinois Consumer Fraud and Deceptive Business Practices Act caused injury to Plaintiffs and Class members. Accordingly, Plaintiffs and the Class are entitled to recover their actual damages from the violation.

122. Defendants also acted with reckless indifference toward the rights of others, such that an award of punitive damages is warranted.

123. Plaintiffs and the Illinois Class members are also entitled to recover their costs of the action, as well as reasonable attorneys' fees.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury for all claims in this Complaint so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class members proposed in this Complaint, respectfully request the following relief:

124. An order certifying the Nationwide Class and Illinois State Class under Federal Rule of Civil Procedure 23, appointing Plaintiffs as Representative of the Class, and appointing the undersigned as Class Counsel;

125. An order enjoining Equifax from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protections of Plaintiffs' and the Classes' data;

126. An order compelling Equifax to employ and maintain appropriate systems and policies to protect consumer data and to promptly detect and timely report any theft or unauthorized access of that data;

127. Actual damages suffered by Plaintiffs and Class members;

128. Punitive damages, as allowable, in an amount determined by the Court or jury;

129. Any and all statutory and enhanced damages;

130. Reasonable and necessary attorneys' fees and costs as provided by statute, common law, or the Court's inherent power;

131. Pre- and post-judgment interest; and

132. Such further relief as the Court deems just and proper.

[signatures continued on next page]

Dated: September 25, 2017
Atlanta, Georgia

Respectfully submitted,

/s/ James E. Butler, Jr.

James E. Butler Jr.
Georgia Bar No. 099625
Joel O. Wooten, Jr.
Georgia Bar No. 776350
Joseph M. Colwell
Georgia Bar No. 531527
Ramsey B. Prather
Georgia Bar No. 658395
BUTLER WOOTEN & PEAK LLP
2719 Buford Highway NE
Atlanta, Georgia 30324
Tel.: (404) 321-1700
Fax: (404) 321-1713
jim@butlerwooten.com
joel@butlerwooten.com
joseph@butlerwooten.com
ramsey@butlerwooten.com

Steven F. Molo*
Justin B. Weiner*
Megan Cunniff Church*
Daniel Michaeli*
MOLO LAMKEN LLP
300 North LaSalle Street
Chicago, Illinois 60654
Tel.: (312) 450-6700
Fax: (312) 450-6701
smolo@mololamken.com
jweiner@mololamken.com
mchurch@mololamken.com
dmichaeli@mololamken.com

Benjamin T. Sirolly*
MOLO LAMKEN LLP
600 New Hampshire Ave. NW
Washington, DC 20037
Tel.: (202) 556-2000
Fax: (202) 556-2001
btsirolly@mololamken.com

Stephen D. Susman*
SUSMAN GODFREY LLP
1000 Louisiana Suite 5100
Houston, Texas 77002
Tel.: (713) 651-9366
Fax: (212) 336-8340
ssusman@susmangodfrey.com

Attorneys for Plaintiffs and the Proposed Classes

* *pro hac vice forthcoming*